Univention Nubus Produktdatenblatt

Nubus gibt Organisationen die Kontrolle über ihre digitale Identitätsinfrastruktur und Geschäftsanwendungen – mit der Flexibilität, diese nach ihren eigenen Vorstellungen zu integrieren und zu betreiben.

Datum: September 2026.

Inhaltsverzeichnis

1 Univention Nubus 2

2 Szenarien / Probleme, die Nubus löst 2

2.2 Zentrales Identitätsmanagement 2
2.3 Authentifizierung, Single Sign-On und Föderation 2
2.4 Zentraler Zugriff auf Anwendungen 3
2.5 Identitätslebenszyklus und Provisionierung 3
2.6 Offene Integrationsplattform 3
2.7 Integration ecosystem 4
2.8 Integration in bestehende Identitätsinfrastrukturen 5
2.9 Flexible Bereitstellung 5
2.10 Skalierbarer und hochverfügbarer Betrieb 5
2.11 Betriebliche Transparenz und Beobachtbarkeit 6
2.12 Transparenz der Software-Lieferkette 6
2.13 Open Source und Betriebskontrolle 6

3 Aktueller Status 7

1 Univention Nubus

Univention Nubus ist eine Open-Source-Plattform für Identity and Access Management zur zentralen Verwaltung digitaler Identitäten und zur Integration von Anwendungen und IT-Systemen. Nubus ist für heterogene IT-Umgebungen und Interoperabilität konzipiert. Anwendungen können über etablierte Standards und dokumentierte APIs integriert werden, während bestehende Identity Provider und Verzeichnisdienste an die zentrale Identitätsinfrastruktur angebunden werden können.

Nubus kann cloud-nativ als Nubus for Kubernetes oder als Nubus for Virtual Machines auf der UCS-Betriebsumgebung betrieben werden. Das Bereitstellungsmodell kann entsprechend der Infrastruktur und den Betriebsanforderungen der Organisation ausgewählt werden.

2 Szenarien / Probleme, die Nubus löst

2.2 Zentrales Identitätsmanagement

Nubus stellt einen zentralen Identitätsspeicher und eine Verwaltungsschicht für digitale Identitäten bereit.

Administratoren können Benutzer, Gruppen, Gruppenmitgliedschaften und Identitätsattribute zentral über eine webbasierte Management-Oberfläche verwalten. Anwendungen und Automatisierungen können über dokumentierte APIs auf Funktionen des Identitätsmanagements zugreifen.

Das Identitätsmodell kann um zusätzliche Attribute erweitert werden, um organisations- und anwendungsspezifische Identitätsinformationen abzubilden.

Damit erhalten Anwendungen eine gemeinsame Identitätsbasis, anstatt jeweils eine eigene unabhängige Benutzer- und Gruppendatenbank verwalten zu müssen.

2.3 Authentifizierung, Single Sign-On und Föderation

Nubus stellt einen zentralen Identity Provider für Authentifizierung und Single Sign-On bereit. Anwendungen können über etablierte Protokolle wie OpenID Connect, OAuth 2.0 und SAML integriert werden. Benutzer können sich zentral authentifizieren und über eine gemeinsame Identität auf integrierte Anwendungen zugreifen.

Nubus kann außerdem mit externen Identity Providern föderiert werden. Bestehende Authentifizierungsinfrastrukturen können daher für die Authentifizierung maßgeblich bleiben, während Nubus die gemeinsame IAM- und Anwendungsintegrationsschicht bereitstellt.

Zwei-Faktor-Authentifizierung wird unterstützt. Nubus bietet außerdem einen 2FA-Helpdesk, über den autorisierte Administratoren die Zwei-Faktor-Anmeldedaten von Benutzern zurücksetzen können; zusätzlich kann eine Self-Service-Zurücksetzung für Benutzer bereitgestellt werden.

2.4 Zentraler Zugriff auf Anwendungen

Das Univention Portal stellt einen zentralen browserbasierten Einstiegspunkt zu Anwendungen und Diensten bereit. Für einen Benutzer verfügbare Anwendungen können in einer gemeinsamen Oberfläche dargestellt werden. Die Inhalte des Portals können auf Grundlage der Gruppenmitgliedschaft gesteuert und an die Organisation angepasst werden.

Nubus bietet außerdem Self-Service-Funktionen für Endbenutzer. Abhängig von Bereitstellung und Konfiguration können Benutzer unterstützte Kontoinformationen pflegen, Passwörter ändern oder zurücksetzen und kontobezogene Aufgaben ohne administrative Intervention durchführen.

Portal, Self Service und Single Sign-On arbeiten auf derselben zentralen Identitätsinfrastruktur.

2.5 Identitätslebenszyklus und Provisionierung

Nubus unterstützt die Weitergabe von Identitätsänderungen an integrierte Anwendungen und Dienste. Der Provisioning Service stellt einen ereignisbasierten Integrationsmechanismus für Systeme bereit, die ihre eigene Datenpersistenz verwalten. Konsumenten können sich für relevante Änderungen an Verzeichnisobjekten registrieren und Benutzer-, Gruppen- und andere identitätsbezogene Änderungen über eine dokumentierte REST-Schnittstelle empfangen.

Dadurch können verbundene Systeme auf Ereignisse des Identitätslebenszyklus reagieren, etwa auf die Erstellung oder Änderung von Benutzern, Änderungen an Gruppenmitgliedschaften oder die Entfernung von Identitäten.

Nubus unterstützt außerdem die initiale Provisionierung von Daten für neu verbundene Konsumenten.

2.6 Offene Integrationsplattform

Nubus ist darauf ausgelegt, Anwendungen verschiedener Anbieter und Technologiestacks zu integrieren. Anstatt einen proprietären Integrationsmechanismus vorauszusetzen, bietet Nubus mehrere Integrationsebenen für unterschiedliche Anwendungsfälle. Dazu gehören:

- OpenID Connect
- OAuth 2.0
- SAML 2.0
- LDAP and LDAPS
- HTTP REST APIs
- UDM HTTP REST API

- SCIM
- ereignisbasierte Provisionierung
- Identitäts- und Anwendungs-Connectoren

Eine Anwendung kann daher nur die von ihr benötigten Funktionen integrieren. Eine Anwendung kann beispielsweise Nubus nur für Single Sign-On verwenden, das zentrale Verzeichnis für Identitätsinformationen nutzen, Ereignisse des Identitätslebenszyklus konsumieren oder mehrere Integrationsmechanismen kombinieren.

Nubus kann auch bestehende IAM- und Verzeichnissysteme anbinden. Der Nubus Directory Importer unterstützt die wiederkehrende unidirektionale Synchronisierung von Benutzern und Gruppen aus externen LDAP-basierten Verzeichnissen nach Nubus. Die Föderation bietet eine Alternative, bei der Identitäten weiterhin von einem externen Identity Provider authentifiziert werden.

2.7 Integration ecosystem

Nubus verbindet allgemeine offene Schnittstellen mit einem etablierten Ökosystem von Anwendungsintegrationen.

Der Univention Integration Catalog bietet eine zentrale Übersicht der für Nubus verfügbaren Integrationen. Er umfasst verschiedene Integrationsmodelle, beispielsweise:

- über offene Standards integrierte Anwendungen
- dokumentierte, konfigurationsbasierte Integrationen
- Identitäts-Connectoren
- Groupware-Connectoren
- paketierte Integrationen
- über das Univention App Center verfügbare Anwendungen
- Integrationen für cloud-native Softwarestacks
- zusätzliche Integrationslösungen von Univention und Ökosystempartnern

Das bedeutet, dass die Integration nicht auf Anwendungen beschränkt ist, für die ein dedizierter Nubus-spezifischer Connector existiert.

Anwendungen, die kompatible Standards wie OpenID Connect, SAML, SCIM oder LDAP unterstützen, können diese Standardschnittstellen verwenden, während komplexere Szenarien des Lebenszyklus oder der Datensynchronisierung dedizierte Integrationskomponenten nutzen können.

Der Integration Catalog dokumentiert den verfügbaren Integrationsweg und die unterstützten Funktionen für einzelne Lösungen.

2.8 Integration in bestehende Identitätsinfrastrukturen

Nubus erfordert nicht, dass Organisationen alle bestehenden Identitätssysteme ersetzen, bevor sie eine gemeinsame IAM-Schicht einführen. Bestehende Identity Provider können über SAML oder OpenID Connect föderiert werden. Bestehende LDAP-basierte Verzeichnisse können über den Nubus Directory Importer angebunden werden.

Nubus for Virtual Machines bietet außerdem umfangreiche Integrationsmöglichkeiten für bestehende Windows-, Linux- und Microsoft-Active-Directory-Umgebungen über die UCS-Betriebsumgebung.

Dadurch kann Nubus in heterogene bestehende Infrastrukturen eingeführt werden und entweder als zentrales Identitätssystem oder als Teil einer föderierten Identitätsarchitektur fungieren.

2.9 Flexible Bereitstellung

Nubus bietet zwei Bereitstellungsmodelle.

Nubus for Kubernetes stellt die IAM-Funktionen als containerisierte Dienste bereit, die mit Kubernetes eingesetzt werden. Die Bereitstellung wird über Helm Charts beschrieben und ist für die Integration in cloud-native Plattformumgebungen ausgelegt.

Nubus for Virtual Machines betreibt die Nubus-IAM-Funktionen auf der UCS-Betriebsumgebung. Es unterstützt die Bereitstellung auf virtuellen Maschinen oder physischen Systemen und bietet zusätzliche Infrastruktur-Funktionen für traditionelle Rechenzentrums- und Domänenumgebungen.

Beide Bereitstellungsvarianten stellen die zentralen Nubus-Funktionen für Identitätsmanagement, Anwendungsintegration, Portal und Single Sign-On bereit. Die im jeweiligen Bereitstellungsmodell verfügbaren detaillierten technischen Funktionen können sich unterscheiden.

2.10 Skalierbarer und hochverfügbarer Betrieb

Nubus ist für den Betrieb in größeren und verteilten Umgebungen ausgelegt.

Nubus for Kubernetes nutzt die Verwaltung von Kubernetes-Workloads, um unterstützte Komponenten zu skalieren. Der Verzeichnisdienst unterstützt getrennte Primary-, Secondary- und Proxy-Rollen. Sekundäre LDAP-Instanzen können für Lese-Workloads skaliert werden, und zwei LDAP-Primary-Instanzen können im Spiegelmodus betrieben werden, um eine hohe Verfügbarkeit des Verzeichnisdienstes bereitzustellen.

Nubus for Virtual Machines unterstützt verteilte Domänenarchitekturen, Verzeichnisreplikation und redundante Verzeichnisknoten.

Die konkrete Architektur für Verfügbarkeit und Skalierung kann daher an das ausgewählte Bereitstellungsmodell und die Betriebsumgebung angepasst werden.

2.11 Betriebliche Transparenz und Beobachtbarkeit

Nubus stellt betriebliche Schnittstellen und Informationen bereit, die in Standardumgebungen für Monitoring und Logging integriert werden können.

Aktuelle Nubus-Releases bieten Schnittstellen für strukturiertes Logging und Metriken. Nubus for Kubernetes kann Metriken für zentrale IAM-Komponenten an Prometheus-kompatible Monitoring-Systeme ausgeben, einschließlich Metriken aus dem Directory Manager und dem Identity Provider.

Technische Informationen zu verwalteten Verzeichnisobjekten, einschließlich Identifikatoren und Änderungsinformationen, stehen Administratoren zur Verfügung.

2.12 Transparenz der Software-Lieferkette

Nubus for Kubernetes stellt Mechanismen bereit, mit denen Betreiber die von Univention bereitgestellten Softwareartefakte verifizieren können.

Container-Images und Helm Charts sind kryptografisch signiert. Informationen zur Software Bill of Materials werden im CycloneDX-Format bereitgestellt, und Informationen zum Vulnerability Exploitability eXchange werden für die Schwachstellenbewertung geliefert.

Diese Mechanismen ermöglichen es Betreibern, Nubus-Artefakte in etablierte Prozesse für Software-Lieferketten und Schwachstellenmanagement zu integrieren.

2.13 Open Source und Betriebskontrolle

Nubus ist Open-Source-Software.

Der Quellcode und – für Nubus for Kubernetes – die Bereitstellungsartefakte sind öffentlich verfügbar. Nubus kann in einer von der Organisation ausgewählten und kontrollierten Infrastruktur betrieben werden, ohne dass die Nutzung einer bestimmten proprietären Identitäts-Cloud erforderlich ist.

Die Verwendung etablierter Protokolle und dokumentierter Schnittstellen unterstützt die Interoperabilität zwischen Open-Source- und proprietären Anwendungen und ermöglicht es Organisationen, ihre IAM-Architektur unabhängig von einem einzelnen Anwendungsanbieter zu gestalten.

3 Aktueller Status

Veröffentlichungsdatum: September 2026.

Für Produktaktualisierungen nach dem Veröffentlichungsdatum dieses Datenblatts wird auf die aktuelle Produktdokumentation und die Release Notes von Univention verwiesen.

Die vollständige und kontinuierlich aktualisierte Dokumentation ist verfügbar unter:

https://docs.software-univention.de/

Sie umfasst die aktuelle Dokumentation für:

- Nubus for Kubernetes Architecture
- Nubus for Kubernetes Operation
- Nubus for Kubernetes Release Notes
- Nubus Manual
- Nubus for Virtual Machines / Nubus for UCS Operation

Die Release Notes dokumentieren neue Funktionen, Änderungen, Fehlerbehebungen, Sicherheitsaktualisierungen, Abkündigungen und Upgrade-Anforderungen für nachfolgende Nubus-Releases.

Für die neuesten Produktfunktionen und technischen Anforderungen sollte die für die jeweils eingesetzte Produktversion geltende Dokumentation herangezogen werden.